Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
wojciech.trabka@uj.edu.pl

Mgr Mariusz Kielar
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

IDENTYFIKACJA i UWIERZYTELNIENIE W SYSTEMIE INFORMACYJNYM OPIEKI ZDROWOTNEJ PO WPROWADZENIU ROZPORZĄDZENIA UE eIDAS

1. Wstęp

Informatyzacja ochrony zdrowia po raz kolejny znalazła się w punkcie wyjścia. Nie wiadomo, czy planowany system w ochronie zdrowia w kształcie przewidzianym ustawą w ogóle ruszy i będzie funkcjonował. W związku z tym należy ponownie rozważyć czy założenia opracowywane przed laty należy wdrażać, czy może rozwiązania technologiczne dnia dzisiejszego umożliwiają inny kształt systemu i jego znaczne uproszczenie oraz odformalizowanie. Nie ulega wątpliwości, że projektowany system oparty na pozyskiwaniu informacji i danych od pacjentów, świadczeniodawców i aptek miał podstawową wadę, która powodowała, że w praktyce nie mógł zostać uruchomiony. Oczywiście chodzi o nieprzygotowanie narzędzi służących do identyfikacji podmiotów w systemie (zarówno świadczących usługi, jak i pacjentów) podpisywania dokumentów

elektronicznych oraz możliwości ich przekazywania, jak również możliwości uwierzytelnia transakcji oraz witryn internetowych. Wszystkie koncepcje dotyczące możliwych do wprowadzenia w życie rozwiązań ostatecznie nie zostały wdrożone. Nie doczekały się wdrożenia koncepcje dowodu osobistego z warstwą elektroniczną, karty specjalisty medycznego i administracyjnego (KSM, KSA) czy też karty pacjenta eKUZ[1].

W chwili obecnej niepewna jest też przyszłość ePUAP[2] wraz z funkcjonującym w ramach platformy podpisem potwierdzonym profilem zaufanym. Od lipca 2016 r. przestaje funkcjonować ustawa o podpisie elektronicznym[3] oraz uregulowany jej przepisami podpis elektroniczny, w tym wykorzystywany w ochronie zdrowia i przez całe lata zalecany i ostatecznie nakazany do stosowania przy prowadzeniu elektronicznej dokumentacji medycznej tzw. bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu.

Warto również zauważyć, że do problemu identyfikacji i uwierzytelnienia odnosi się Dyrektywa Parlamentu Europejskiego i Rady 011/24/UE. Przewiduje ona utworzenie sieci organów krajowych odpowiedzialnych za e-zdrowie. Aby zwiększyć bezpieczeństwo i ciągłość transgranicznej opieki zdrowotnej, sieć musi opracować wytyczne w sprawie transgranicznego dostępu do danych i usług związanych z e-zdrowiem, również poprzez wspieranie „wspólnych środków identyfikacji i uwierzytelniania, aby ułatwić przenoszalność danych w transgranicznej opiece zdrowotnej". Zapewnienie wzajemnego uznawania elektronicznej identyfikacji i uwierzytelniania jest niezbędne, aby urzeczywistnić transgraniczną opiekę zdrowotną dla obywateli Europy. Gdy obywatele wyjeżdżają w celu podjęcia leczenia ich dane

[1] W § 3, ust. 1 Zarządzenia Ministra Zdrowia z dnia 25 marca 2014 r. w sprawie powołania Zespołu do spraw wdrożenia karty ubezpieczenia zdrowotnego i karty specjalisty medycznego zapisano, że do zadań Zespołu należy m.in.: 1) przygotowanie rozwiązań w zakresie funkcjonalności elektronicznej karty ubezpieczenia zdrowotnego (eKUZ) i 2) karty specjalisty medycznego (KSM) oraz 3) infrastruktury Narodowego Funduszu Zdrowia (Infrastruktura Klucza Publicznego) i świadczeniodawców - bezpieczne czytniki umożliwiające złożenie podpisu elektronicznego za pomocą *eKUZ i KSM;* Dz. Urz. Min. Zdr. 2014.50 ogłoszony: 2014-03-26

- W projekcie ustawy o zmianie ustawy z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia z 30 kwietnia 2015 r. zakładano trzy rodzaje kart elektronicznych i związanych z nimi systemów teleinformatycznych:
1) karty ubezpieczenia zdrowotnego (KUZ)
2) karty specjalisty medycznego (KSM),
3) karty specjalisty administracyjnego (KSA).

[2] Wypowiedzi Minister Cyfryzacji A. Streżyńskiej po kolejnych awariach platformy http://www.dobreprogramy.pl/Po-kolejnej-awarii-ePUAP-moze-jednak-czas-zaorac-eadministracyjny-niewypal,News,72952.html

[3] Zostanie uchylona w drodze art. 125 ustawy o usługach zaufania oraz identyfikacji elektronicznej.

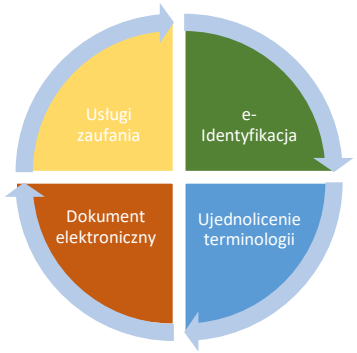
medyczne muszą być dostępne w kraju, w którym prowadzone jest leczenie. Wymaga to stworzenia solidnych, bezpiecznych i wiarygodnych ram identyfikacji elektronicznej.

W tej sytuacji należy spróbować odpowiedzieć na pytanie, jaka jest najbliższa przyszłość narzędzi służących do identyfikacji i uwierzytelnienia oraz składania podpisów, pieczęci elektronicznych, jak też innych usług zaufania niezbędnych zarówno do prowadzenia i przetwarzania dokumentacji medycznej prowadzonej w postaci elektronicznej, obsługi systemu informacji w ochronie zdrowia oraz innych usług związanych z wykorzystaniem systemów informatycznych i sieci telekomunikacyjnych, w tym usług z zakresu telemedycyny.

W tym roku wchodzi w życie Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z dn. 28 sierpnia 2014 r.)[4] – zwany dalej elDAS. Jest to akt prawny obowiązujący na terenie Unii Europejskiej bezpośrednio i nie wymagający implementacji prawa krajowego (Rysunek 1). Jednak w przypadku tej regulacji w kilku obszarach pozostawiono swobodę dla prawa krajowego. W związku z tym, przygotowuje się ustawę o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw.[5]

Celem artykułu jest wskazanie co wynika z powyższych regulacji w praktyce funkcjonowania systemu opieki zdrowotnej.

Rysunek 1. Obszary regulacji eIDAS



Źródło: Opracowanie własne.

[4] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910
[5] https://legislacja.rcl.gov.pl/projekt/12283556, Projekt ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw

Identyfikacja elektroniczna w ochronie zdrowia w świetle Rozporządzenia eIDAS i projektu przepisów krajowych.

Zgodnie z definicją zawartą w Polskiej Normie[6] identyfikacja to proces zautomatyzowanego rozpoznania określonego użytkownika w systemie możliwy do zrealizowania dzięki zastosowaniu unikalnych nazw.

Obecnie w ochronie zdrowia mamy codziennie do czynienia z koniecznością identyfikacji pacjenta, jak i osoby świadczącej usługi medyczne. W przypadku pacjenta weryfikacja jego tożsamości i uprawnień następuje w trakcie wizyty na podstawie dowodu osobistego i systemu EWUŚ. Pacjent ma również możliwość sprawdzenia uprawnień m.in. lekarza[7] czy diagnosty[8] w rejestrach, przed wizytą lub po jej zakończeniu. Dodatkowo, jeżeli pacjent nie ma możliwości sprawdzenia w rejestrze, może dokonać sprawdzenia u kierownika podmiotu świadczącego usługi lecznicze. Osoby kierujące instytucjami świadczącymi usługi zdrowotne są zobowiązane do sprawdzania uprawnień osób zatrudnianych, co w rezultacie pozwala pacjentowi domniemywać, że ma do czynienia z osobą uprawnioną[9].

Wiele usług w sektorze publicznym realizowanych jest *online*. Dotyczy to także sektora opieki zdrowotnej. Usługi takie realizowane są w różnym zakresie w wielu krajach Unii Europejskiej. Celem identyfikacji elektronicznej dla potrzeb realizacji usług *online* jest umożliwienie posiadaczowi środka identyfikacji elektronicznej wydanego w jednym kraju członkowskim, możliwości skorzystania z publicznych usług *online* w innych krajach członkowskich. Wiele usług *online* nie musi bowiem wymagać użycia podpisu elektronicznego – wystarczy, że osoba fizyczna posługująca się określonymi danymi umożliwiającymi jej jednoznaczną identyfikacją zostanie dobrze i bez wątpliwości rozpoznana przez system teleinformatyczny i będzie mogła skorzystać z szeregu usług, jakie są w ramach tego systemu oferowane, w szczególności nie

[6] PN-I-020003.1.031
[7] Art. 50 ust.1 Ustawa z dnia 2 grudnia 2009 r. o izbach lekarskich Dz.U. 2009 nr 219 poz. 1708
[8] Art.8 ustawy z dnia 27 lipca 2001 r., o diagnostyce laboratoryjnej (tj. Dz. U. 2014 poz. 174).
[9] Art. 108 ust. 2 pkt 3 ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej. Dz.U. 2011 nr 112 poz. 654

podpisując dokumentów elektronicznych tylko wydając określone dyspozycje, jako uwierzytelniony w systemie użytkownik[10].

W przypadku ochrony zdrowia, przy usługach świadczonych *online*, prawidłowa identyfikacja podmiotów biorących w nich udział w zasadzie warunkuje możliwość ich świadczenia np. przy usługach z zakresu telekonsultacji. Pacjent musi mieć pewność, że ma do czynienia rzeczywiście z osobą uprawnioną, nie pozbawioną prawa wykonywania zawodu (system powinien również rozpoznawać stan po wyroku, a przed jego uprawomocnieniem), oraz że osoba nieuprawniona nie posługuje się skradzioną tożsamością.

Równie ważna jest identyfikacja podmiotów świadczących usługi nie będących osobami fizycznymi. Identyfikator potwierdza, czy podmiot świadczący usługi świadczy je zgodne z ich zakresem określonym w odpowiednim rejestrze, a tym samym, czy ma możliwość świadczenia danej usługi zdrowotnej.

Ponadto poprawna identyfikacja umożliwia pacjentowi m.in. dostęp *online,* zapisywanie się na wizyty, czy weryfikację określonych informacji zawartych w rejestrach np. informację o zarejestrowaniu podmiotu leczniczego i tym samym o możliwości świadczenia przez dany podmiot usług zdrowotnych.

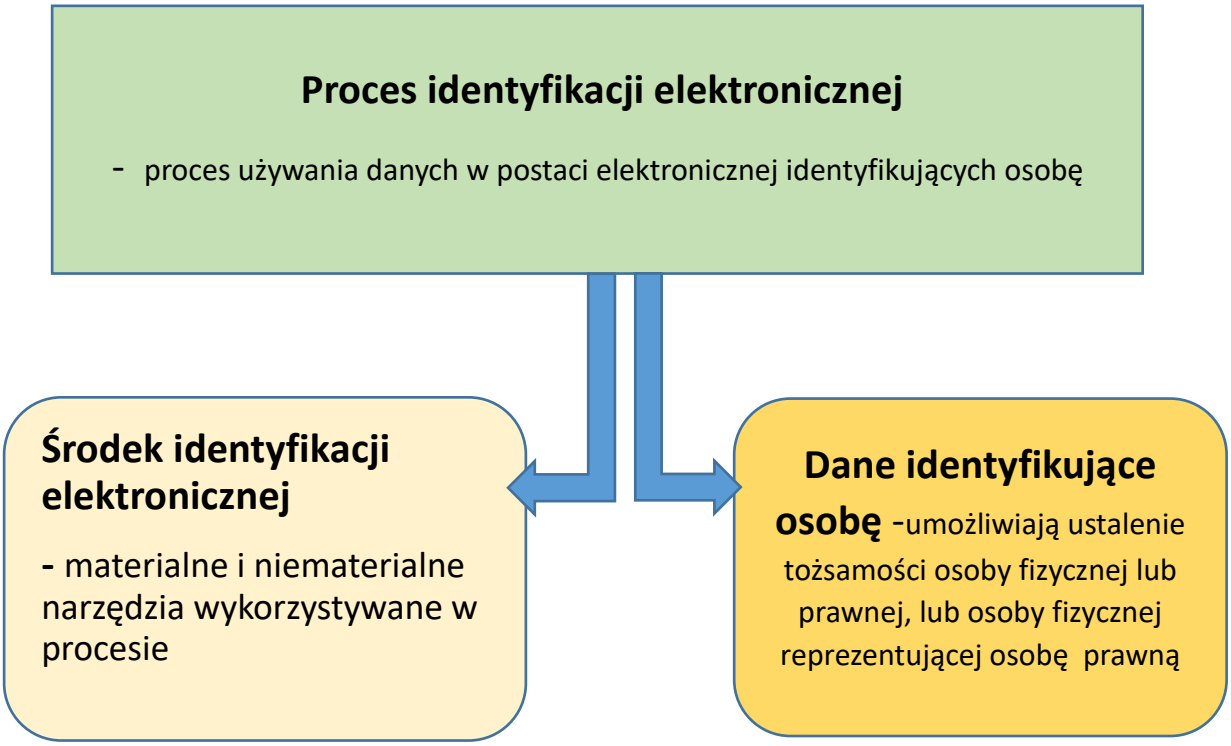
Identyfikacja elektroniczna eID.

W rozumieniu eIDAS identyfikacja elektroniczna tzw. elD oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną lub osobę fizyczną reprezentującą osobę prawną[11]. Uzupełnieniem tej definicji jest definicja przyjęta na potrzeby Rozporządzenia projektu STORK[12]**.** Identyfikacja to proces pozyskania informacji od deklarowanej tożsamości (strony) bez uwzględnienia wiarygodności tej informacji[13].

[10] Uzasadnienie projektu ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw

[11] Art. 3 ust.1 Rozporządzenia eIDAS
[12] W ramach projektu STORK stworzono już założenia ramowe elektronicznej tożsamości https://www.eid-stork.eu/index.php?optio
[13] STORK - D2.3 - *Quality authenticator scheme*

Rysunek 2. Elementy procesu identyfikacji elektronicznej wg Rozporządzenia eIDAS



Źródło: Opracowanie własne

W procesie identyfikacji następuje deklaracja tożsamości podmiotu. W celu umożliwienia identyfikacji wydaje się często materialne narzędzia umożliwiające ten proces – np. dowód osobisty lub karty identyfikacyjne w instytucjach (Rysunek nr 2). Obecnie dawne np. dowody osobiste, czy identyfikatory zastępowane są przez takie, które umożliwiają identyfikację elektroniczną.

Środek identyfikacji elektronicznej oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi *online*[14]. Inaczej mówiąc, środki wykorzystywane w procesie identyfikacji

[14] Art. 3 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

mogą mieć postać materialną (np. Karta KUZ) lub niematerialną (np. odpowiednie oprogramowanie w smartfonie czy warstwa elektroniczna karty identyfikacyjnej). Środek identyfikacji jednoznacznie identyfikuje osobę zarówno fizyczną jak i prawną i stanowi elektroniczną tożsamość użytkownika w tymże środowisku. Sama identyfikacja pozwala zatem na stwierdzenie „o kogo chodzi", ale nie potwierdza, że użytkownik danej e-usługi jest faktycznie tą osobą, która została zadeklarowana i zidentyfikowana. Do tego potwierdzenia służy uwierzytelnienie polegające na dostarczeniu dowodów, że użytkownik jest właśnie tą zidentyfikowaną osobą („nikt się nie podszywa")[15]. Rozporządzenie definiuje „uwierzytelnianie" jako proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej[16].

Projektowana zmiana ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[17] określa, że uwierzytelnienie użytkowników systemu teleinformatycznego, korzystających z usług *online* udostępnianych przez podmioty realizujące zadania publiczne, wymaga:

- użycia notyfikowanego środka identyfikacji elektronicznej, adekwatnie do poziomu bezpieczeństwa wymaganego dla usług świadczonych w ramach tych systemów, lub
- profilu zaufanego ePUAP lub
- danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego.

Wszystkie działania związane z przygotowaniem systemu identyfikacji elektronicznej (również w ochronie zdrowia) muszą uwzględnić bezpośrednio obowiązujące na terenie danego kraju przepisy prawa. Naszym zdaniem, obok przygotowania i wdrożenia środków identyfikacji, należy uporządkować wszystkie

[15] Mielnici T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013

[16] Artykuł 3 ust.5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

[17] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565 zmiany przewiduje Art. 95. o usługach zaufania oraz identyfikacji elektronicznej Projekt z dnia 03.06.2016 r. zmiana art. 20 a

uregulowane prawnie usługi możliwe do realizacji online oraz umożliwić dostęp do ich wykazu wszystkim zainteresowanym. Dostęp bowiem do tych usług i ich ostateczne wykonanie na rzecz wnioskodawcy odbywać się musi na warunkach określonych w przepisach danego kraju. Wynika z tego, że np. usługi z zakresu telemedycyny mogą być świadczone w niektórych krajach UE na podstawie krajowych regulacji poszczególnych krajów (np. Norwegii[18]).

Bezpieczeństwo i transgraniczność eID

Zapewnienie bezpieczeństwa systemu eID jest warunkiem koniecznym przy opracowywaniu założeń identyfikatorów służących do przetwarzania danych medycznych (tzw. danych wrażliwych) zawartych m.in w warstwie elektronicznej projektowanej Karty Ubezpieczenia Zdrowotnego KUZ (w związku z przewidywanymi zmianami ustrojowymi w systemie ochrony zdrowia nazwa identyfikatora zostanie zmieniona; zmieni się również jego zastosowanie).

Obecnie istnieje konieczność takiego zaprojektowania systemu identyfikacji w ochronie zdrowia, który powinien uwzględniać także identyfikatory notyfikowane w krajach UE oraz możliwość wykorzystywania narzędzi identyfikacyjnych do korzystania między innymi z systemów informacyjnych ochrony zdrowia w krajach UE.

Projektowany system eID musi zapewnić bezpieczeństwo jego użytkownikom - w szczególności, jeżeli wykorzystywany jest do przetwarzania danych o stanie zdrowia. System identyfikacji elektronicznej na poziomie kraju - w tym również na poziomie krajowego systemu opieki zdrowotnej – musi zapewnić bezpieczeństwo podmiotu identyfikacyjnego tj. obejmującego:

- prawidłową weryfikację deklarowanej tożsamości osób,
- weryfikację prawidłowości przyporządkowania danej osoby i jej tożsamości do określonych uprawnień wynikających z dokumentu, jakim się ona posługuje,

[18] Zanaboni P., Knarvik U., Wootton R., *Adoption of routine telemedicine in Norway: the current Picture*, Glob Health Action 2014, **7:** 22801 - http://dx.doi.org/10.3402/gha.v7.22801

- obrót prawny i gospodarczy związany z użyciem dokumentów potwierdzających tożsamość lub określone uprawnienia,
- ochronę obywateli przed kradzieżą tożsamości.[19]

Problematyką identyfikacji elektronicznej zajmuje się rozdział II Rozporządzenia eIDAS. Uregulowano tam między innymi:

- wzajemne uznawanie i akceptowanie środków identyfikacji elektronicznej;
- warunki notyfikowania systemów identyfikacji elektronicznej oraz zapewnienia im interoperacyjności technicznej;
- poziomy bezpieczeństwa systemów identyfikacji elektronicznej;
- naruszenia bezpieczeństwa systemów identyfikacji elektronicznej;
- odpowiedzialność notyfikującego państwa członkowskiego;
- współpracę państw członkowskich i zapewnienia ram interoperacyjności dla systemów identyfikacji elektronicznej.

Jednym z celów eIDAS jest zniesienie, w przypadku usług publicznych, istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uwierzytelniania. Przyjęto zasadę o nieingerowaniu w systemy zarządzania tożsamością elektroniczną i w powiązane z nimi infrastruktury ustanowione w państwach członkowskich. Pozostawiono swobodę w stosowaniu lub wprowadzaniu środków dostępu do usług online do celów identyfikacji elektronicznej, oraz swobodę w podjęciu decyzji, czy w dostarczanie tych środków należy zaangażować sektor prywatny. Jednak w przeciwieństwie do usług zaufania publicznego tworzenie i obsługę systemów identyfikacji elektronicznej powierzono organom państw członkowskich.

Generalnie uznano, że państwo, a nie komercyjne firmy, jest uznawane za wiarygodny podmiot mogący gwarantować poprawność np. certyfikatów, tym bardziej, że zwykle dysponuje już wiarygodnym i pełnym rejestrem obywateli[20]. System zarządzania tożsamością powinien opierać się na cyfrowych certyfikatach

[19] Lewandowski R., *Elektroniczna karta ubepieczenia zdrowotnego - słabe i mocne strony projektowanego rozwiązania.* http://ww1.pwpw.pl/kwartalnik_archiwum.html?id=48&magCid=249
[20] Papińska-Kacperek J., *Usługi cyfrowe. Perspektywy wdrożenia i akceptacji cyfrowych usług administracji publicznej w Polsce*. Wydawnictwo Uniwersytetu Łódzkiego, 2013

gwarantowanych przez państwo i np. zawartych w nowych dokumentach tożsamości. Nie we wszystkich krajach zdecydowano się na ten wariant. W niektórych wyposaża się obywateli w elektroniczne dowody osobiste lub inne dokumenty umożliwiające identyfikację tylko w komunikacji z urzędami, czasami nie we wszystkich sprawach. Nie wszędzie nowe dokumenty zawierają dane biometryczne, a podpis cyfrowy jest najczęściej opcjonalny. Dokumenty wykorzystujące dane biometryczne (twarz/odcisk palca) wykorzystywane są m.in. w Niemczech, Holandii, Hiszpanii. Dokumenty umożliwiające ich wykorzystywanie w ochronie zdrowia posiada m.in. Austria, Belgia, Portugalia. W Estonii i Włoszech karty umożliwiają składanie podpisu elektronicznego[21].

Po pozytywnym wykorzystaniu systemów bankowych w projekcie „Rodzina 500 plus" nie wykluczono wykorzystania przez Polskę systemów bankowych.[22] Systemy te bowiem są od wielu lat wykorzystywane i akceptowane przez obywateli. W Estonii logowanie do portalu www.esti.ee, odpowiednika polskiego ePUAP, odbywa się, albo za pomocą elektronicznego dowodu, albo poprzez system bankowy. Użytkownik loguje się jak do swojego banku, ale zostaje zachowana poufność działań, tzn. bank i urząd nie mają dostępu do danych drugiej instytucji. Podobne rozwiązanie wprowadzane jest w Danii. Przyczyną było małe zainteresowanie usługą adekwatną do profilu zaufanego: po wielu latach jej funkcjonowania skorzystało z niej tylko 20% obywateli. Z tego powodu duński rząd z bankami utworzył centralny system identyfikacji NemID. Wykorzystanie systemów bankowych wdrażane jest również w Kanadzie i USA. *Canada's Cyber Authentication Renewal* wykorzystuje rozwiązania uwierzytelniania wdrożone przez banki, wydawców kart kredytowych, urzędy i podmioty świadczące opiekę zdrowotną. Usługa uwierzytelniania *SecureKey* pozwala uzyskać dostęp do usług rządowych przy użyciu danych potrzebnych do logowania w serwisach banków lub, jeśli bank na to zezwoli, przez mikroprocesorową kartę płatniczą. Usługa *Secure- Key Credential Broker*

[21] Tamże

[22] 95% wniosków zostało wypełnionych z wykorzystaniem systemów kilkunastu banków "Rodzina 500+": wnioski online składane głównie przez banki. Zobacz najczęstsze błędy http://www.polskieradio.pl/42/273/Artykul/1603800,Rodzina-500-wnioski-online-skladane-glownie-przez-banki-Zobacz-najczestsze-bledy.

Service (CBS) została wdrożona w USA w 2012 roku. Być może takie uwierzytelnienie będzie stosowane także w naszym kraju.[23]

System zarządzania tożsamością.

W ostatnim czasie uregulowano warunki organizacyjne i techniczne, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników.[24] *Zdefiniowano i określono właściwości zarządzania tożsamością oraz niezbędne czynności, które muszą być zrealizowane przy zarządzaniu systemem.*

System zarządzania tożsamością to system teleinformatyczny, przetwarzający informacje o tożsamości użytkowników i wykorzystywany przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne metody niż certyfikat.

System zarządzania tożsamością posiada następujące właściwości:

- rejestruje użytkowników;
- potwierdza tożsamość użytkowników;
- przechowuje i udostępnia dane identyfikacyjne użytkowników systemom autoryzującym uprawnionym do ich otrzymania;
- umożliwia zablokowanie konta użytkownika na jego żądanie;
- zapewnia rozliczalność;
- zapewnia integralność, autentyczność i poufność danych identyfikacyjnych i uwierzytelniających użytkownika;
- zapewnia codzienną synchronizację czasu systemowego z czasem UTC(PL).

Administrowanie systemem zarządzania tożsamością wymaga realizowania następujących czynności:

- zapewniania wiarygodności procesu rejestracji użytkowników i potwierdzania ich tożsamości;

[23] Papińska-Kacperek J., *Usługi cyfrowe. Perspektywy wdrożenia i akceptacji cyfrowych usług administracji publicznej w Polsce*. Wydawnictwo Uniwersytetu Łódzkiego, 2013

[24] Projekt rozporządzenia Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników – https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

- przechowywania informacji dotyczących tożsamości użytkownika przez okres 20 lat, licząc od dnia 1 stycznia roku następnego od chwili wykonania w systemie ostatniej operacji z użyciem tożsamości;
- utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, zapewniającej jego bezpieczną eksploatację;
- opracowania i wdrożenia polityki zarządzania bezpieczeństwem informacji.

Te podmioty, które zdecydują się na opracowanie i wdrożenie polityki zarządzania bezpieczeństwem informacji, dla której wymagania bezpieczeństwa określono zgodne z Polską Normą[25] spełniają wymagania określone powyżej.

System autoryzujący i certyfikujący

Zdefiniowano ponadto *system autoryzujący, jako system teleinformatyczny używany przez podmiot publiczny, który wykorzystuje usługi systemu certyfikującego lub systemu zarządzania tożsamością do przeprowadzenia procesu uwierzytelniania użytkownika*[26].

System autoryzujący identyfikując użytkownika dokonuje weryfikacji tożsamości i przechowuje dane potwierdzające tę weryfikację.

Dane potwierdzające weryfikację, powinny w sposób jednoznaczny umożliwiać:

- identyfikację tożsamości osoby, która dokonała czynności w postaci elektronicznej;
- stwierdzenie ważności uprawnień w momencie dokonania czynności;
- ustalenie czasu dokonania czynności.

Zdefiniowano również pojęcie systemu certyfikującego,[27] rozumianego jako system teleinformatyczny służący do wydawania certyfikatów wykorzystywanych przez

[25] PN ISO/IEC 27001:2007 lub nowszą, zweryfikowana pozytywnie przez jednostkę certyfikującą akredytowaną, zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. poz. 542).

[26] § 2 pkt.3 Projekt rozporządzenia Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników – https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

[27] § 2 pkt.1 Projekt rozporządzenia Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników – https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

podmioty publiczne do uwierzytelniania użytkowników. Określono również jego właściwości. System ten:

- świadczy usługi niezwłocznego unieważnienia certyfikatu;
- precyzyjnie określa czas wystawienia i unieważnienia certyfikatu
- potwierdza tożsamość osoby, dla której jest wydawany certyfikat;
- spełnia wymagania w zakresie bezpieczeństwa teleinformatycznego, dobierane na podstawie analizy ryzyka;
- nie gromadzi ani nie kopiuje danych służących użytkownikom do identyfikacji z wykorzystaniem certyfikatów.

Administrowanie systemem certyfikującym wymaga realizowania następujących czynności:

- systematycznego przeglądu skuteczności zastosowanych środków w zakresie bezpieczeństwa teleinformatycznego, w celu wprowadzania ich usprawnień;
- utrzymywania w stanie aktualnym dokumentacji operacyjnej i technicznej systemu, zapewniającej jego bezpieczną eksploatację;
- zapewniania organizacyjnego, technicznego i kryptograficznego bezpieczeństwa działania systemu;
- przeciwdziałania fałszowaniu certyfikatów, w tym zapewniania poufności podczas procesu tworzenia danych do potwierdzania tożsamości;
- przechowywania informacji dotyczących wydanych certyfikatów przez okres 20 lat, licząc od dnia 1 stycznia roku następnego po ich wytworzeniu;
- informowania osób ubiegających się o certyfikat o warunkach stosowania certyfikatu, w szczególności o ograniczeniach użycia certyfikatu i postępowaniu w przypadku skarg i rozstrzygania sporów.

Powyższe wymagania mogą być spełnione, gdy została wdrożona odpowiednia polityka certyfikacji,[28] zapewnione zostały odpowiednie warunki organizacyjne i techniczne,[29] oraz wykorzystano zgodne ze standardami systemy i produkty.[30]

Wzajemne uznawanie i notyfikacja Komisji Europejskiej.

Wprowadzono zasadę wzajemnego uznawania w stosunku do systemów identyfikacji elektronicznej notyfikowanych przez państwa członkowskie, które spełniły warunki notyfikacji i notyfikacja ta została opublikowana w Dzienniku Urzędowym Unii Europejskiej. Zasada wzajemnego uznawania odnosi się wyłącznie do uwierzytelniania dla usługi *online*.

Nie ma obowiązku notyfikowania Komisji swoich systemów identyfikacji elektronicznej. Decyzję o tym, czy notyfikować Komisji wszystkie, niektóre lub żaden z systemów identyfikacji elektronicznej używanych na szczeblu krajowym dla uzyskiwania dostępu przynajmniej do publicznych usług, online lub szczególnych usług pozostawiono państwom członkowskim.

Jeżeli, zgodnie z prawem krajowym lub zgodnie z krajową praktyką administracyjną, dostęp do usługi online świadczonej przez podmiot sektora publicznego w jednym państwie członkowskim wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, w tym pierwszym państwie członkowskim na potrzeby transgranicznego uwierzytelnienia dla tej usługi online uznaje się środek identyfikacji elektronicznej wydany w innym państwie członkowskim, pod warunkiem, że spełnione są następujące warunki:

- środek identyfikacji elektronicznej jest wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję
- poziom bezpieczeństwa środka identyfikacji elektronicznej odpowiada poziomowi bezpieczeństwa równemu lub wyższemu od poziomu bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na

[28] Spełniająca wymagania wskazane w standardzie ETSI TS 102 042 w wersji 1.2.4. lub nowszym;
[29] Zgodne z wymaganiami standardu CWA 14167-1 lub nowszego w zakresie świadczenia usług innych niż wydawanie certyfikatów kwalifikowanych;
[30] Zgodne z wymaganiami standardu CWA 14167-2, 3 i 4 lub nowszego

potrzeby dostępu do tej usługi online w pierwszym państwie członkowskim, pod warunkiem, że poziom bezpieczeństwa tego środka identyfikacji elektronicznej odpowiada średniemu lub wysokiemu poziomowi bezpieczeństwa;

- odpowiedni podmiot sektora publicznego korzysta ze średniego lub wysokiego poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi *online*.

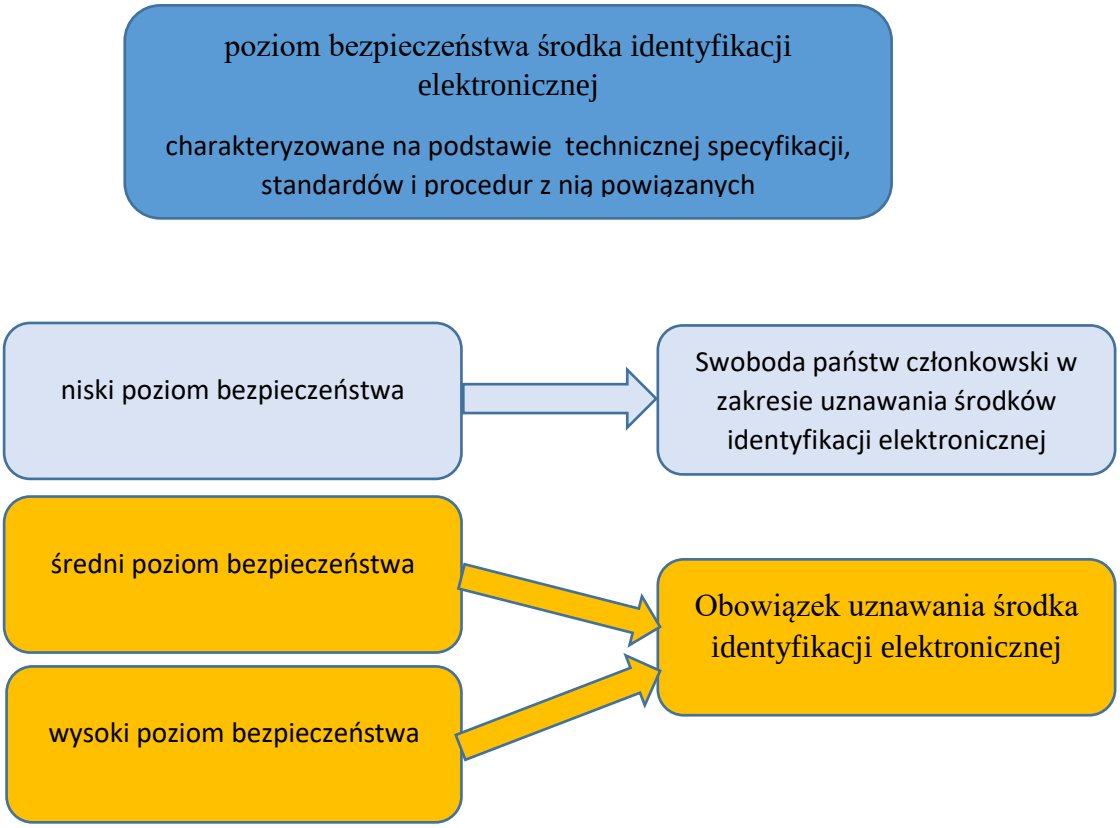
Obowiązek uznawania środka identyfikacji elektronicznej powinien odnosić się wyłącznie do tych środków, których poziom bezpieczeństwa tożsamości jest równy poziomowi wymaganemu w odniesieniu do danej usługi *online* lub wyższy od tego poziomu. Ponadto obowiązek ten powinien mieć zastosowanie wyłącznie wtedy, gdy dany podmiot sektora publicznego używa „średniego" lub „wysokiego" poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi *online*.

Pozostawiono swobodę państwom członkowskim w zakresie uznawania środków identyfikacji elektronicznej charakteryzujących się niższymi poziomami bezpieczeństwa.

Poziom bezpieczeństwa.

System identyfikacji elektronicznej określa niski, średni lub wysoki poziom bezpieczeństwa, w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach tego systemu. Poziomy bezpieczeństwa powinny oznaczać stopień, w jakim można mieć zaufanie do środka identyfikacji elektronicznej przy ustalaniu tożsamości danej osoby, dając tym samym pewność, że osoba podająca daną tożsamość jest faktycznie osobą, której przypisano tę tożsamość. Zależy od stopnia zaufania, jaki ten środek identyfikacji elektronicznej zapewnia co do podawanej lub zgłaszanej tożsamości danej osoby, przy uwzględnieniu procesów (na przykład potwierdzanie i weryfikacja tożsamości oraz uwierzytelnianie), działań zarządczych (na przykład jednostka wydająca środek identyfikacji elektronicznej i procedura wydawania takiego środka) oraz stosowanych zabezpieczeń technicznych.

Rysunek 3. Poziomy bezpieczeństwa środka identyfikacji elektronicznej



Źródło: Opracowanie własne

Poziom bezpieczeństwa uzależniony jest od rodzaju danych, do których mamy dostęp. Inne wymagania odnoszą się do dostępu do wrażliwych danych medycznych, inne do pobierania formularzy urzędowych. W zależności od rodzaju usługi i wymaganego poziomu bezpieczeństwa zastosowane powinny być adekwatne metody i techniki uwierzytelnienia o określonej wiarygodności. W związku z tym, dla każdej usługi powinien zostać określony (na podstawie analizy ryzyka) poziom wiarygodności wymagany dla procesu uwierzytelnienia. Poziom wiarygodności określa stopień zaufania dopuszczalny i akceptowalny biorąc pod uwagę straty, jakie mogą być poniesione w przypadku błędnego uwierzytelnienia. Dla ułatwienia porównań usług i metod uwierzytelnienia oraz uzyskania interoperacyjności powstały różne klasyfikacje standaryzujące poziomy wiarygodności i ich interpretację, wraz z wymaganiami co do

procesów i technik w zakresie identyfikacji i uwierzytelnienia[31]. Do określania powyższych procesów opracowano normę ISO 29115. Opisano w niej cztery poziomy wiarygodności od minimalnego do wysokiego (Rysunek 3).

Dostępność systemów identyfikacji dla sektora prywatnego

System identyfikacji tworzony jest głównie z myślą o sektorze publicznym. Lecz nie ma przeszkód, aby umożliwić dobrowolne korzystanie z systemu przez sektor prywatny, gdy identyfikacja jest potrzebna do celów usług *online* lub transakcji elektronicznych.

W Polsce wprowadza się zmiany[32], które wychodzą naprzeciwko powyższym postulatom. W przygotowywanym projekcie rozporządzenia Ministra Cyfryzacji w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej określono warunki organizacyjne i techniczne nieodpłatnego wykorzystywania w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy. Wykorzystanie w ePUAP środków identyfikacji elektronicznej stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, realizowane będzie na podstawie porozumienia zawartego pomiędzy ministrem a podmiotem niepublicznym.

Jednak wykorzystanie w ePUAP środków identyfikacji elektronicznej, stosowanych do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, wymaga:

[31] Mielnicki T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013

[32] Projekt rozporządzenia Ministra Cyfryzacji w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej Projekt 03.06.2016 r.

- wdrożenia przez podmiot niepubliczny zabezpieczeń dotyczących co najmniej średniego poziomu zaufania[33],
- opracowania i ustanawiania, wdrażania i eksploatowania, monitorowania i przeglądania oraz utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji;
- poddawania się przez podmiot niepubliczny audytowi sprawdzającemu spełnienie wymagań, przez niezależną trzecią stronę, nie rzadziej niż raz w roku;
- potwierdzenia przez podmiot niepubliczny tożsamości osoby, której udostępniono środki identyfikacji elektronicznej stosowane do uwierzytelniania w systemie teleinformatycznym podmiotu niepublicznego, na podstawie:
    - okazanego podczas osobistego stawiennictwa dowodu osobistego albo paszportu zawierającego numer PESEL,
    - danych pochodzących z poprawnie przeprowadzonej weryfikacji kwalifikowanego podpisu elektronicznego, przy użyciu którego osoba ta podpisała dokument elektroniczny, w którym oświadczyła, iż świadoma jest warunków i zalecanych środków zaufania związanych z korzystaniem z systemu identyfikacji elektronicznej oraz wyraziła zgodę na nadanie statusu użytkownika tego systemu oraz wykorzystywanie udostępnionych środków identyfikacji elektronicznej w systemie ePUAP.

Platforma ePUAP może wymieniać informacje z innymi systemami teleinformatycznymi podmiotów realizujących zadania publiczne oraz systemami podmiotów niepublicznych. Przewidziano możliwość uzyskania certyfikatu dla systemu teleinformatycznego na wniosek podmiotu niepublicznego.

Aby ułatwić transgraniczne korzystanie z takich środków identyfikacji elektronicznej przez sektor prywatny, możliwość uwierzytelniania zapewniona przez jakiekolwiek państwo członkowskie powinna być dostępna dla stron ufających[34] z sektora prywatnego, mających siedzibę poza terytorium tego państwa członkowskiego, na tych samych warunkach co warunki stosowane do stron ufających z sektora prywatnego

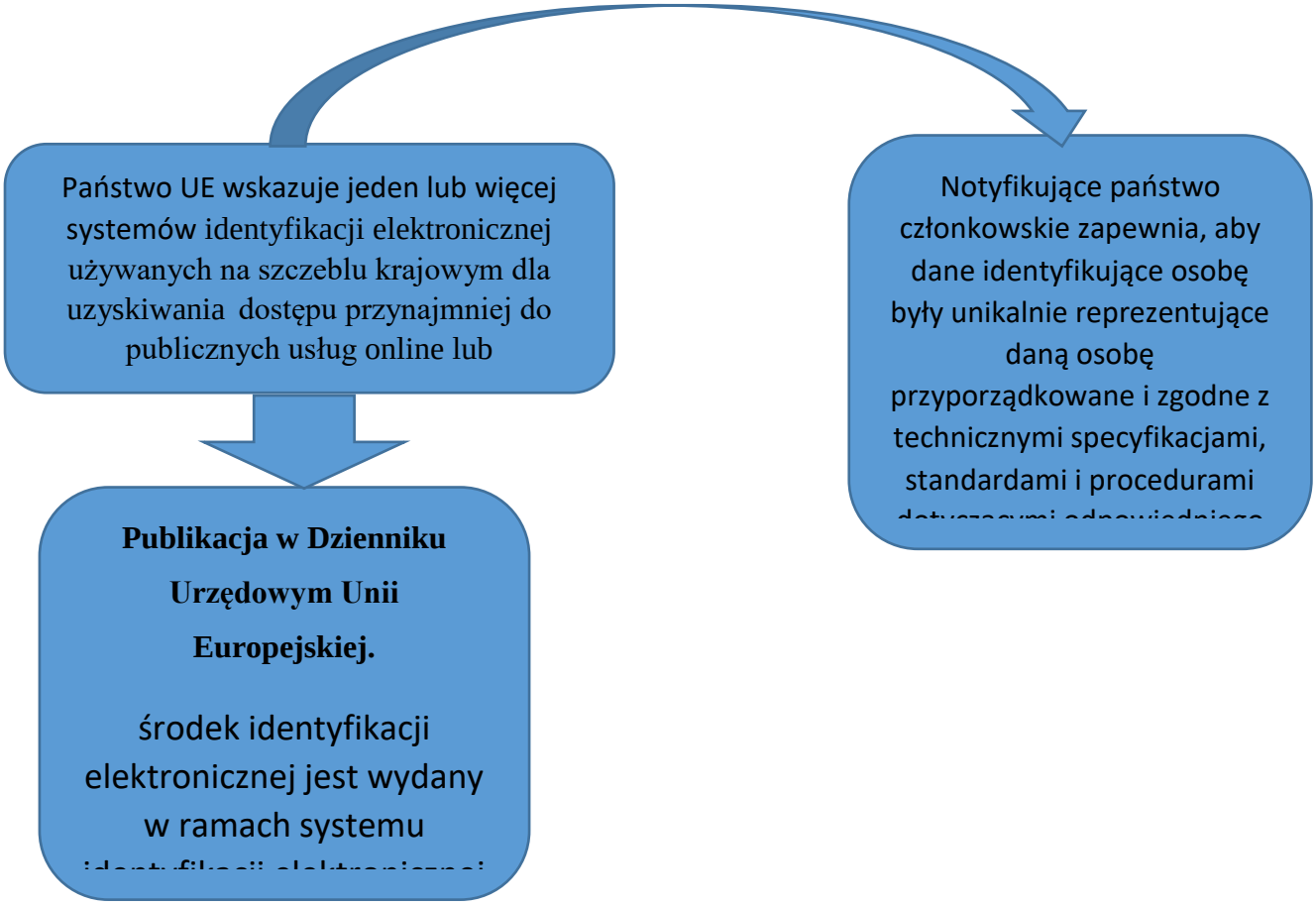
[33] Wymaganych rozporządzeniem wykonawczym Komisji (UE)2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych

[34] Strona ufająca oznacza osobę fizyczną lub prawną, która podlega identyfikacji elektronicznej lub usłudze zaufania;

mających siedzibę na terytorium tego państwa członkowskiego. Państwo członkowskie może określić warunki dostępu do środków uwierzytelniania oraz poinformować, czy środki uwierzytelniania powiązane z notyfikowanym systemem są obecnie dostępne dla stron ufających z sektora prywatnego.

Środek identyfikacji elektronicznej, który jest wydawany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję, który odpowiada niskiemu poziomowi bezpieczeństwa, może być uznany przez podmioty sektora publicznego na potrzeby transgranicznego uwierzytelniania dla usługi online świadczonej przez te podmioty (Rysunek 4).

Rysunek 4. System identyfikacji elektronicznej w Unii Europejskiej



Źródło: Opracowanie własne

Trwają prace koncepcyjne nad opracowaniem krajowego identyfikatora. Poprzez powszechny, „narodowy" identyfikator rozumie się tutaj identyfikator, który jest:

- dostępny dla szerokich mas obywateli, potencjalnie dla wszystkich dorosłych,
- posiadany masowo,
- wydawany przez państwo lub uznawany przez państwo (w przypadku wydawców komercyjnych),
- dostępny dla e-usług zarówno publicznych, jak i komercyjnych,
- wiarygodny ("bezpieczny"),
- interoperacyjny.

W Polsce początkowo rozważano wprowadzenie elektronicznego dowodu tożsamości (projekt pl.ID). Po wycofaniu się z projektu rozważano do notyfikacji dwa projekty Profilu Zaufanego w ramach eIDAS. Drugim systemem planowanym przez Polskę do notyfikacji jest Karta Ubezpieczenia Zdrowotnego „KUZ." Przygotowania odbywały się w ramach projektu „Ariadna". Główny cel projektu to wdrożenie rozporządzenia eIDAS z uwzględnieniem narodowego dorobku w obszarze wewnątrzadministracyjnym, tj. usług ePUAP, Profilu Zaufanego oraz innych usług zaufania w administracji publicznej. Projekt zakłada wykorzystanie ePUAP, jak również Profilu Zaufanego oraz innych istniejących rozwiązań informatycznych już dostępnych a ułatwiających realizację przedmiotowego celu. Wydzielony Profil Zaufany będzie dostarczał mechanizmy potwierdzenia tożsamości i uwierzytelniania obywateli Polski po przeprowadzeniu procesu notyfikacji. Profil Zaufany będzie skomunikowany (dwukierunkowo) z ogólnokrajowym serwisem PEPSem, od którego będzie przyjmował żądania identyfikacji, a do którego będzie wysyłał potwierdzenia - lub brak takowego - tożsamości obywatela[35].

W projekcie ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw przewidziano utworzenie krajowego węzła elDAS[36], czyli punktu

[35] Załącznik nr 8 do Studium Wykonalności projektu „Ariadna" - Dostosowanie Profilu Zaufanego do unijnych wymogów rozporządzenia elDAS, https://mac.gov.pl/files/zalacznik_nr_8_kopia_protokolu_z_prezentacji_publicznej_ariadna.pdf

[36] W Rozporządzeniu wykonawczym komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności wydanym na podstawie art. 12 ust. 8 elDAS projekt ustawy o identyfikacji i usługach zaufania Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowego węzła identyfikacji eIDAS

przyłączenia umożliwiającego sprzężenie krajowej infrastruktury identyfikacji elektronicznej w Polsce z krajowymi infrastrukturami państw UE. Krajowy węzeł identyfikacji elDAS będzie pełnił podwójną rolę:

- będzie pośredniczył w uwierzytelnianiu posiadaczy zagranicznych środków identyfikacji elektronicznej wydanych w ramach notyfikowanych systemów identyfikacji w krajowych usługach *online*,
- będzie pośredniczył w uwierzytelnianiu posiadaczy krajowych środków identyfikacji elektronicznej w zagranicznych usługach *online*, w przypadku gdy system identyfikacji, w ramach którego środki tego zostały wydane, będzie notyfikowany do identyfikacji elektronicznej innych państw członkowskich[37].

Reasumując, krajowy węzeł eIDAS będzie stanowił niezbędną podstawę do notyfikowania polskiego systemu identyfikacji elektronicznej, bez względu na to, jaki system zostanie wskazany.

Literatura:

[1.] Papińska-Kacperek J., *Usługi cyfrowe. Perspektywy wdrożenia i akceptacji cyfrowych usług administracji publicznej w Polsce*. Wydawnictwo Uniwersytetu Łódzkiego, 2013
[2.] Lewandowski R., *Elektroniczna karta ubezpieczenia zdrowotnego - słabe i mocne strony projektowanego rozwiązania*. Źródło internetowe: http://ww1.pwpw.pl/kwartalnik_archiwum.html?id=48&magCid=249
[3.] Mielnicki T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013
[4.] PN ISO/IEC 27001:2007
[5.] PN-I-020003.1.031
[6.] Projekt rozporządzenia Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników – źródło internetowe: https://legislacja.rcl.gov.pl/docs//522/12286305/12357434/12357435/dokument225309.pdf

[37] Projekt ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw – źródło internetowe: https://legislacja.rcl.gov.pl/projekt/12283556

[7.] Projekt ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw – źródło internetowe: https://legislacja.rcl.gov.pl/projekt/12283556
[8.] Projekt ustawy o zmianie ustawy z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia z 30 kwietnia 2015 r.
[9.] Rozporządzenie wykonawcze Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności – źródło internetowe: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015R1501
[10.] Rozporządzenie wykonawcze Komisji (UE)2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych – źródło internetowe: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015R1501
[11.] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
[12.] Standard CWA 14167-1 w zakresie świadczenia usług innych niż wydawanie certyfikatów kwalifikowanych;
[13.] Standard ETSI TS 102 042, wersja 1.2.4.
[14.] STORK - D2.3 - *Quality authenticator scheme*
[15.] Ustawa z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku, Dz.2016 U. poz. 542
[16.] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, Dz.U. 2011 nr 112 poz. 654
[17.] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565
[18.] Ustawa z dnia 2 grudnia 2009 r. o izbach lekarskich, Dz.U. 2009 nr 219 poz. 1708
[19.] Ustawa z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej, Dz. U. 2014 poz. 174.
[20.] Załącznik nr 8 do Studium Wykonalności projektu „Ariadna" - Dostosowanie Profilu Zaufanego do unijnych wymogów rozporządzenia elDAS" https://mac.gov.pl/files/zalacznik_nr_8_kopia_protokolu_z_prezentacji_publicznej_ariadna.pdf
[21.] Zanaboni P., Knarvik U., Wootton R, *Adoption of routine telemedicine in Norway: the current Picture*, Glob Health Action 2014, **7:** 22801 - http://dx.doi.org/10.3402/gha.v7.22801
[22.] Zarządzenia Ministra Zdrowia z dnia 25 marca 2014 r. w sprawie powołania Zespołu do spraw wdrożenia karty ubezpieczenia zdrowotnego i karty specjalisty medycznego, Dz. Urz. Min. Zdr. 2014.50 ogłoszony: 2014-03-26;
[23.] Źródło internetowe: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910
[24.] Źródło internetowe: http://www.dobreprogramy.pl/Po-kolejnej-awarii-ePUAP-moze-jednak-czas-zaorac-eadministracyjny-niewypal,News,72952.html
[25.] Źródło internetowe: http://www.polskieradio.pl/42/273/Artykul/1603800,Rodzina-500-wnioski-online-skladane-glownie-przez-banki-Zobacz-najczestsze-bledy.

[26.] Źródło internetowe: https://legislacja.rcl.gov.pl/projekt/12283556, Projekt ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw

Streszczenie:

Informatyzacja ochrony zdrowia po raz kolejny znalazła się w punkcie wyjścia. Nie wiadomo czy planowany system w ochronie zdrowia w kształcie przewidzianym ustawą w ogóle ruszy i będzie funkcjonował. W związku z tym, należy ponownie rozważyć, czy założenia opracowywane przed laty należy wdrażać, czy może rozwiązania technologiczne dnia dzisiejszego umożliwiają inny kształt systemu i jego znaczne uproszczenie i odformalizowanie.

Należy spróbować odpowiedzieć na pytanie, jaka jest najbliższa przyszłość narzędzi służących do identyfikacji i uwierzytelnienia oraz składania podpisów, pieczęci elektronicznych, jak też innych usług zaufania, niezbędnych zarówno do prowadzenia i przetwarzania dokumentacji medycznej prowadzonej w postaci elektronicznej, rozwiązań systemu krajowego oraz innych usług związanych z wykorzystaniem systemów informatycznych i sieci telekomunikacyjnych, w tym usług z zakresu telemedycyny.

W 2016 roku wchodzi w życie Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z dn. 28 sierpnia 2014 r.) – elDAS. Jest to akt prawny obowiązujący na terenie Unii Europejskiej bezpośrednio i nie wymagający implementacji prawa krajowego. Jednak w przypadku tej regulacji w kilku obszarach pozostawiono swobodę dla prawa krajowego. W związku z tym przygotowuje się ustawę o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw.

Celem artykułu jest wskazanie, co wynika z powyższych regulacji w praktyce funkcjonowania systemu opieki zdrowotnej.